Discrete Mathematics 310 (2010) 3188–3193

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On the spectrum of the sizes of semiovals in PG(2, q), q odd

György Kiss [a,b], Stefano Marcugini [c], Fernanda Pambianco [c,*]

[a] Department of Geometry, Eötvös Loránd University, H-1117 Budapest, Pázmány s. 1/c, Hungary

[b] Bolyai Institute, University of Szeged, H-6720 Szeged, Aradi vértanúk tere 1, Hungary

[c] Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, 06123 Perugia, Italy

ARTICLE INFO

Article history:
Received 30 September 2008
Received in revised form 1 July 2009
Accepted 27 July 2009
Available online 11 August 2009

Keywords:
Projective planes
Semiovals

ABSTRACT

Some characterization theorems and non-existence results of semiovals with extra properties are proved. New examples of large semiovals are constructed for $q = 11$ and $q = 13$.

1. Introduction

Let Π be a projective plane of order q. A *semioval* in Π is a non-empty pointset $\mathcal{S}$ with the property that for every point P in $\mathcal{S}$ there exists a unique line t_P such that $S \cap t_P = \{P\}$. This line is called the tangent to $\mathcal{S}$ at P. The classical examples of semiovals arise from polarities (ovals and unitals), and from the theory of blocking sets (the vertexless triangle). The semiovals are interesting objects in their own right, but the study of semiovals is also motivated by their applications to cryptography [2].

It is known that $q + 1 \leq |\mathcal{S}| \leq q\sqrt{q} + 1$ and both bounds are sharp [11,19]; the extremes occur when $\mathcal{S}$ is an oval or a unital, respectively. The sizes of the known semiovals are close to either the upper, or the lower bound; almost nothing is known about semiovals for which $3q - 2 \leq |\mathcal{S}| \leq q\sqrt{q}$ holds. Large semiovals can be constructed as unions of conics if q is an odd square, applying a method developed by Hirschfeld and Szőnyi [10]. In Section 2 we generalize their method for $q \equiv 1 \pmod 4$. We prove that in PG(2, q) there is a semioval of size s for all $q\lceil 4 \log q \rceil < s \leq q\sqrt{q} + 1$ if q is an odd square. In Section 3 we present some new examples of medium size semiovals for $q \leq 13$. These semiovals were found by computer search.

If $|\mathcal{S}| = q + 1$ or $|\mathcal{S}| = q\sqrt{q} + 1$, then all nontangent lines intersect $\mathcal{S}$ in either 0 or a points, where $a = 2$ or $\sqrt{q} + 1$, respectively. Semiovals with this extra property are called regular with character a. Recently Gács [8] proved that in PG(2, q) each regular semioval is either an oval or a unital. Semiovals which have only three intersection sizes 1, $m + 1$ and $n + 1$ with the lines of the plane, were studied by Batten and Dover [3]. They found only one example for $q \leq 1024$: this is a cyclic semioval in PG(2, 7). We prove some non-existence results about cyclic semovals in Section 4.

Semiovals with large collinear subsets were investigated by Dover [7]. He proved, that a semioval contains at most $q - 1$ points of a line if $q > 3$ and if S has a $(q-1)$-secant, then $|S| = 2q-2$, or $2q \leq |S| \leq 3(q-1)$. If S has more than one $(q-1)$-secant and $q \geq 7$, then S can be obtained from a vertexless triangle by removing some subsets of points from one side. Some examples of semiovals having $(q - 2)$-secants were found by Suetake [17]. In Section 4 we prove some characterization theorems about semiovals having $(q - 2)$-secants.

* Corresponding author. Tel.: +39 075 585 5006; fax: +39 075 585 5024.
E-mail address: fernanda@dipmat.unipg.it (F. Pambianco).

0012-365X/$ – see front matter
doi:10.1016/j.disc.2009.07.024

2. Semiovals contained in the union of conics

Throughout this section let α be a fixed nonsquare element of GF(q), and for $a \in$ GF(q) let $\mathcal{P}_a$ be the conic in PG(2, q) with equation

$$\mathcal{P}_a: \quad X_2X_3 = X_1^2 + \alpha a X_3^2.$$

If q is an odd square, then Hirschfeld and Szőnyi [10] and independently Baker and Ebert [1] constructed a unital in PG(2, q) as union of $\sqrt{q}$ conics. Let us briefly summarize their construction.

Consider the pencil of superosculating conics $\{\mathcal{P}_a : a \in \mathrm{GF}(q)\}$. Let $\{a_1, a_2, \ldots, a_{\sqrt{q}}\}$ be the elements of GF($\sqrt{q}$) $\subset$ GF(q). Then the subset of this pencil

$$\mathcal{U} = \bigcup_{i=1}^{\sqrt{q}} \mathcal{P}_{a_i}$$

is a unital. If a point $R \in \mathcal{P}_{a_i}$, then the tangent line to $\mathcal{U}$ at R is the same as the tangent line to $\mathcal{P}_{a_i}$ at R. In particular, the tangent line to $\mathcal{U}$ at $Y_\infty(0, 1, 0)$ is the line with equation $X_3 = 0$. If this line is considered as the line at infinity, ℓ_∞, then on the affine plane PG(2, q) $\setminus \ell_\infty$ these conics are the parabolas with equation $Y = X^2 + \alpha a_i$.

It follows from their construction, that any subset of $1 \le k \le \sqrt{q}$ conics

$$\mathcal{S} = \bigcup_{j=1}^{k} \mathcal{P}_{a_{i_j}}$$

forms a semioval of size $kq+1$. If q is a square, then $q \equiv 1 \pmod 4$. Semiovals which are the union of conics can be constructed for all q satisfying $q \equiv 1 \pmod 4$. The following theorem is an easy consequence of a result of Szőnyi ([18], Theorem 1 and Proposition 2).

Theorem 1. *Let $q \equiv 1 \pmod 4$. If $\{a_1, a_2, \ldots, a_k\} \subset GF(q)$ is a subset of $k \ge 2$ elements such that $a_i - a_j$ is a square for all $i \ne j$, then the sets*

$$\mathcal{S} = \bigcup_{i=1}^{k} \mathcal{P}_{a_i} \quad \text{and} \quad \mathcal{S}_1 = \bigcup_{j=1}^{k} \mathcal{P}_{a_j} \setminus \{Y_\infty\}$$

are semiovals of size $kq + 1$ and kq, respectively.

Corollary 2. *Let $q \equiv 1 \pmod 4$, and let c_q be the cardinality of the largest clique in the Paley graph P_q. Then PG $(2, q)$ contains semiovals of size kq and of size $kq + 1$ for all $k = 2, 3, \ldots, c_q$.*

Proof. Let $\{a_1, a_2, \ldots, a_{c_q}\}$ be a maximal clique in P_q. Then $a_i - a_j$ is a square for all $i \ne j$, hence the statement follows from Theorem 1. ■

The cardinality of maximal cliques of Paley graphs were investigated by several authors. We refer to the results of Cohen [6]: if q is a square, then the elements of GF($\sqrt{q}$) form the maximal clique. If q is a nonsquare, then the best known lower bound on the size of a maximal clique is approximately $\log_2 q/2$. Hence Theorem 1 gives the following.

Corollary 3. *Let $q \equiv 1 \pmod 4$ be a nonsquare. Then PG $(2, q)$ contains semiovals of size kq and of size $kq + 1$ for $k = 2, 3, \ldots, \lfloor \log_2 q/2 \rfloor$.*

The semiovals of size $q\lfloor \log_2 q/2 \rfloor + 1$ are the largest known semiovals in these planes so far. We mention that these semiovals are minimal blocking sets, too, see [18].

We can construct new semiovals from existing ones by careful deletion of some points.

Definition 1. A semioval $\mathcal{S}$ is k-fat, if it has no i-secants for $i = 2, 3, \ldots, k - 1$.

Proposition 4. *Let $\mathcal{S}$ be a k-fat semioval. If $\mathcal{T} \subset \mathcal{S}$ has the property that each line meets $\mathcal{T}$ in at most $k - 2$ points, then $\mathcal{S} \setminus \mathcal{T}$ is a semioval.*

Proof. Let R be a point of $\mathcal{S} \setminus \mathcal{T}$. Then the tangent to $\mathcal{S}$ at R is obviously a tangent to $\mathcal{S} \setminus \mathcal{T}$ at R. The only thing what we have to prove is that no new tangents appear after the deletion of points of $\mathcal{T}$. But if a line ℓ meets $\mathcal{S}$ in more than one point, then $|\mathcal{S} \cap \ell| \ge k$, because $\mathcal{S}$ is k-fat. Hence $|(\mathcal{S} \setminus \mathcal{T}) \cap \ell| \ge k - (k - 2) = 2$. Thus no former secant becomes a tangent line to $\mathcal{S} \setminus \mathcal{T}$. ■

Theorem 5. *Let q be an odd square and m be an integer satisfying*

$$q\frac{\sqrt{q}+1}{2} \le m \le q\sqrt{q} + 1.$$

Then PG $(2, q)$ contains semiovals of size m.

Proof. Let $a_1, a_2, \ldots, a_{\sqrt{q}}$ be the elements of GF($\sqrt{q}$). We construct a semioval of size m by deleting some points from the set

$$\mathcal{U} = \bigcup_{i=1}^{\sqrt{q}} \mathcal{P}_{a_i}.$$

This set is a unital, hence it is a $(\sqrt{q}+1)$-fat semioval.

If $m = kq$ or $m = kq+1$ for an integer k, then the statement follows from Corollary 2. Otherwise, consider the unique integer k for which $kq < m < (k+1)q$ holds. It follows, from our assumption, that $k \geq (\sqrt{q}+1)/2$. Let $\mathcal{T}_1$ be the set of points of $\sqrt{q}-k-1$ parabolas, $\cup_{i=k+2}^{\sqrt{q}} \mathcal{P}_{a_i}$ except the point Y_∞, and let $\mathcal{T}_2$ be the set of any $(k+1)q-m$ points of $\mathcal{P}_{a_{k+1}}$. Then $\mathcal{T} = \mathcal{T}_1 \cup \mathcal{T}_2$ is contained in the union of $\sqrt{q}-k$ conics, hence each line meets it in at most $2(\sqrt{q}-k) \leq \sqrt{q}-1$ points, because any line contains at most 2 points of a conic.

Thus $\mathcal{S} \setminus \mathcal{T}$ is a semioval by Proposition 4, and its cardinality is $q\sqrt{q} - (\sqrt{q}-k-1)q - ((k+1)q-m) = m$. ■

We can prove the existence of much smaller semiovals using a theorem about dominating sets of bipartite graphs. Let A and B be the two vertex subsets of a bipartite graph. We say that a vertex $v \in B$ dominates the subset $S \subset A$, if for any $s \in S$ there is an edge between v and s. A subset $B' \subset B$ is a dominating set, if for any $a \in A$ there exists $b' \in B'$ which dominates a. The following lemma is due to S. K. Stein, the proof can be found e.g. in [9].

Lemma 6. *Let A and B be the two vertex subsets of a bipartite graph. Denote by d the minimum degree in A. If A has at least two elements, then there is a set $B' \subset B$ dominating the vertices of A with*

$$|B'| \leq \left\lceil |B| \frac{\log(|A|)}{d} \right\rceil$$

where log *denotes the natural base logarithm.*

Theorem 7. *Let q be an odd square and m be an integer satisfying*

$$q\lceil 4\log q\rceil + 1 \leq m \leq q\sqrt{q}+1$$

where log *denotes the natural base logarithm. Then PG $(2, q)$ contains semiovals of size m.*

Proof. Let $a_1, a_2, \ldots, a_{\sqrt{q}}$ be the elements of GF($\sqrt{q}$). We prove that the unital

$$\mathcal{U} = \bigcup_{i=1}^{\sqrt{q}} \mathcal{P}_{a_i}$$

contains a semioval of size m.

We define a bipartite graph with two vertex subsets A and B. Let the vertices in B be the parabolas of $\mathcal{U}$, and the vertices in A be those lines that are not tangents to $\mathcal{U}$. Let $a \in A$ and $b \in B$ be joined if and only if the corresponding line is a bisecant of the corresponding parabola. Then $|B| = \sqrt{q}$, $|A| = q^2 - q\sqrt{q} + q$ and $d = (\sqrt{q}+1)/2$. Hence from Lemma 6 we get that there exists $B' \subset B$ dominating A, and

$$|B'| \leq \left\lceil |B| \frac{\log(|A|)}{d} \right\rceil = \left\lceil \sqrt{q} \frac{\log(q^2 - q\sqrt{q} + q)}{(\sqrt{q}+1)/2} \right\rceil \leq \lceil 4\log q\rceil.$$

Thus there exists a subset of $\lceil 4\log q\rceil$ parabolas $\mathcal{V} \subset \mathcal{U}$ such that each secant of $\mathcal{U}$ meets $\mathcal{V}$ in at least two points. Hence $\mathcal{V}$ is a semioval of size $s = q\lceil 4\log q\rceil + 1$.

If $m > s$, then consider the unique integer k for which $kq < m - s \leq (k+1)q$ holds. It follows from our assumption, that $0 \leq k \leq \sqrt{q} - \lceil 4\log q\rceil$. Let $\mathcal{T}$ be the union of k parabolas from the set $\mathcal{U} \setminus \mathcal{V}$, $\mathcal{W}$ be a parabola from the set $\mathcal{U} \setminus (\mathcal{V} \cup \mathcal{T})$ and let $\mathcal{W}_1$ be an arbitrary set of $m - s - kq$ points of $\mathcal{W} \setminus Y_\infty$. Then $\mathcal{S} = \mathcal{V} \cup \mathcal{T} \cup \mathcal{W}_1 \subset \mathcal{U}$ is a semioval of size m, because each secant of the semioval $\mathcal{U}$ meets it in at least two points. ■

The following theorem shows that we cannot construct small semiovals by the simple expedient of deleting some points from the union of two superosculating conics if they are internal to each other.

Theorem 8. *Let $q \equiv 1 \pmod 4$. If a semioval $\mathcal{S}$ in PG $(2, q)$ is contained in $\mathcal{P}_a \cup \mathcal{P}_b$ where $a - b$ is a square in GF (q), then $|\mathcal{S}|$ is either $2q$ or $2q+1$.*

Proof. If we do not delete any point, or if we delete only the point Y_∞, then we get semiovals of size $2q+1$ or $2q$, respectively.

Suppose that $\mathcal{S}$ does not contain a point $D_1 \in (\mathcal{P}_a \cup \mathcal{P}_b) \setminus \{Y_\infty\}$. Without loss of generality we may assume that $b = 0$ and $D_1 \in \mathcal{P}_a$.

D_1 is an internal point of $\mathcal{P}_0$, hence there are $(q+1)/2$ external lines to $\mathcal{P}_0$ through D_1. After the deletion of D_1, each of these lines is a tangent to $\mathcal{P}_a \cup \mathcal{P}_0 \setminus \{D_1\}$. One of these lines is the original tangent to $\mathcal{S}$ at D_1, but each of the remaining

$(q-1)/2$ lines contains one more point of $\mathcal{P}_a$. Thus $(q-1)/2$ points of $\mathcal{P}_a$, say $D_2, D_3, \dots D_{(q+1)/2}$, do not belong to $\mathcal{S}$. Replacing D_1 by D_i for $i = 2, 3, \dots, (q+1)/2$, there are two possibilities: either the number of affine points in $\mathcal{P}_a \setminus \mathcal{S}$ is larger than $(q+1)/2$, or the set $\mathcal{D} = \{D_1, D_2, \dots D_{(q+1)/2}\}$ has the property that each line joining two points of $\mathcal{D}$ is disjoint from $\mathcal{P}_0$.

In the former case a simple counting argument shows that there are more than one tangent to $\mathcal{S}$ through each of the remaining points of $\mathcal{P}_a$.

Suppose that we deleted exactly $(q+1)/2$ points, the elements of the set $\mathcal{D}$. Let the affine coordinates of D_i be $(d_i, d_i^2+\alpha a)$. The line D_iD_j is disjoint from $\mathcal{P}_0$. Then the equation

$$X^2 = (d_i + d_j)X - d_i d_j + \alpha a \tag{1}$$

has no roots. Hence $(d_i - d_j)^2 + 4\alpha a$ is a nonsquare for all i, j.

Consider in PG$(2, q)$ the irreducible conic $\mathcal{C}$ having equation $X_1^2 + 4\alpha a X_3^2 = X_2^2$. It has two ideal points $(\pm 1, 1, 0)$, hence it has $q-1$ affine points. The line $X_2 = 0$ is an exterior line of $\mathcal{C}$, because $4\alpha a$ is a nonsquare, while the affine point $(x, y, 1)$ is on $\mathcal{C}$ if and only if the affine point $(x, -y, 1)$ is on $\mathcal{C}$. Hence the affine equation $X^2 + 4\alpha a = Y^2$ has $q-1$ solutions (x, y), and x takes $(q-1)/2$ distinct values among the solutions. Thus if $(d_i - d_j)^2 + 4\alpha a$ is a nonsquare for all i, j, then $(d_i - d_j)$ must take the remaining $q - (q-1)/2 = (q+1)/2$ values for all i, j.

Let $D = \{d_1, d_2, \dots, d_{(q+1)/2}\}$, $-D = \{-d_1, -d_2, \dots, -d_{(q+1)/2}\}$, and consider the set $D + (-D)$ in the additive group of GF(q). By the Theorem of Kneser (see [16], page 6), there exists a subgroup H such that $D + (-D) = D + (-D) + H$ and $|D + (-D)| \geq |D + H| + |(-D) + H| - |H|$. Hence

$$\frac{q+1}{2} = |D + (-D)| \geq |D + H| + |(-D) + H| - |H| \geq \frac{q+1}{2} + \frac{q+1}{2} - |H|.$$

This implies $|H| \geq (q+1)/2$, so $|H| = q$. But this means that $|D + (-D)| = q$, so each element of GF(q) can be written as $d_i - d_j$ for suitable i, j. It means that Eq. (1) has some roots. This contradiction finishes the proof. ■

For small values of q there are semiovals contained in the union of three conics of a pencil of superosculating conics. We found such examples by computer search in the planes of order 25 and 49.

3. On the spectrum of sizes for $q \leq 13$.

Semiovals of size $2(q-1)+k$ for all $0 \leq k \leq q-1$ and $k \neq 1$ can be constructed easily. If we delete any set of $q-1-k$ points from one side of a vertexless triangle, then the remaining points form a semioval $\mathcal{S}$, and $|\mathcal{S}| = 2(q-1)+k$. Hence the spectrum of sizes always contains $2q-2$ and all integers in the interval $[2q, 3q-3]$. For $q \leq 9$, q odd, Lisonek [15] determined the spectrum by exhaustive computer search. He proved the following theorem.

Theorem 9. *The spectrum of the sizes of semiovals in PG* $(2, q)$ *is the following:*

- *If* $q = 3$ *then* $|\mathcal{S}| \in \{4, 6\}$.
- *If* $q = 5$ *then* $|\mathcal{S}| \in \{6, 8, 9, 10, 11, 12\}$.
- *If* $q = 7$ *then* $|\mathcal{S}| \in \{8, 9, 12, 13, 14, 15, 16, 17, 18, 19\}$.
- *If* $q = 9$ *then* $|\mathcal{S}| \in \{10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28\}$.

The number of projectively distinct classes of each size is also known for $q \leq 7$, see [13]. We have also found examples of the following sizes:

Theorem 10.
- *In PG* $(2, 11)$ *there are semiovals of size* $12, 15, 20$, *and for each integer* s *satisfying* $22 \leq s \leq 34$.
- *In PG* $(2, 13)$ *there are semiovals of size* $14, 18, 24$, *and for each integer* s *satisfying* $26 \leq s \leq 40$.

The theoretical upper bounds in these planes are 37 and 47, respectively. For $q = 17$ the size of the largest known semioval is 52, while the upper bound is 71. So if we consider the big semiovals, then the gap between the theoretical upper bound and the size of the largest known one increases.

The smallest size for which there exists an infinite family other than the ovals, is $3(q-1)/2$. It was constructed by Kiss and Ruff [14]. It is easy to prove, that if a semioval contains at least $(q-1)/2$ collinear points, or an oval (properly) if q is odd, then the semioval has at least $3(q-1)/2$ points. These facts together with the result of our computer search, support the following conjecture.

Conjecture 11. *If a semioval in PG* $(2, q)$, $q > 7$, *has less than* $3(q-1)/2$ *points, then it has exactly* $q+1$ *points and it is an oval.*

4. The exceptional semiovals in PG(2, 7)

There are some interesting semiovals in PG(2, 7). The first one has only $q+2$ points. If $q = 7$, then $q + 2 = 3(q-1)/2$, and the semioval belongs to an infinite class of semiovals. The following classification theorem is a consequence of a result of Blokhuis [4].

Theorem 12. *If $|\mathcal{S}| = q + 2$, q odd, then $q = 7$. $\mathcal{S}$ is projectively equivalent to the set of points $\{(0, 1, s), (s, 0, 1), (1, s, 0) : s$ is a square in GF(7)$\}$, hence it is contained in a vertexless triangle.* ■

There is no known infinite class of semiovals of size $2q-1$. There are only four known semiovals of this size; they appear on the planes of order 5, 7, 8 and 9. The following theorem characterizes the case $q = 7$.

Theorem 13. *If $|\mathcal{S}| = 2q - 1$ and $\mathcal{S}$ has a $(q-2)$-secant, then $q = 7$ and $\mathcal{S}$ has exactly two $(q-2)$-secants.*

Proof. If $q \leq 13$, then the statement follows from our exhaustive computer search. Let us suppose that $q \geq 17$. It was proved by Kiss ([12], Theorem 1.1), that if $\mathcal{S}$ is a semioval in PG$(2, q)$, there exist integers t and k such that $|\mathcal{S}| \leq 2q - t + k$, $2(t + k) \leq q$, $t + 4(k + 1) \leq q$ and $\mathcal{S}$ has a $(q - t)$-secant, then the tangent lines of S at the points of the $(q - t)$-secant are concurrent. In our case $t = 2$ and $k = 2$ satisfy the conditions if $q \geq 17$ holds hence the tangent lines of $\mathcal{S}$ at the points of the $(q - 2)$-secant are concurrent.

Let now ℓ be a $(q-2)$-secant of $\mathcal{S}$, P_1, P_2 and P_3 be the three points of $\ell \setminus \mathcal{S}$, and let C be the common point of the tangent lines of $\mathcal{S}$ at the points of ℓ. Then each of the $q + 1$ points of $\mathcal{S} \setminus \ell$ is contained in $\cup_{i=1}^{3} CP_i$. Let $|CP_i \cap \mathcal{S}| = m_i$ for $i = 1, 2, 3$. Then $m_i \leq m_j + m_k$ if $\{i, j, k\} = \{1, 2, 3\}$, because if $R \in CP_i \cap S$, then one of the two lines RP_j and RP_k is not tangent to $\mathcal{S}$, thus $\mathcal{S}$ must contain at least one of the points $RP_j \cap CP_k$ and $RP_k \cap CP_j$. This implies $m_i \leq (q+1)/2$. Without loss of generality we may assume that $m_1 \leq m_2 \leq m_3$, so $(q + 1)/4 \leq m_2$ and $(q + 1)/3 \leq m_3$.

Consider now the points of $\mathcal{S} \cap \ell$. There is a unique tangent of $\mathcal{S}$ through each point, hence there are $(q-1)$ lines through each point which meet $\cup_{i=1}^{3} CP_i \cap \mathcal{S}$. Thus there are at most two lines through each point of $\mathcal{S} \cap \ell$ that meet $\cup_{i=1}^{3} CP_i \cap \mathcal{S}$ in more than one point, hence the total number of such lines is at most $2(q-2)$. But the lines joining the points in $CP_2 \cap \mathcal{S}$ and those in $CP_3 \cap \mathcal{S}$ are pairwise distinct and each of them meets $\ell \setminus \{P_2, P_3\}$. The number of these lines is m_2m_3, and at most m_2 of them contains P_1. So there are at least $m_2(m_3 - 1)$ lines through the points of $\mathcal{S} \cap \ell$ that meet $\cup_{i=1}^{3} CP_i \cap \mathcal{S}$ in more than one point. We prove that $m_2(m_3 - 1) > (q+1)^2/9 - (q+1)/3$. It is obvious if $m_2 > (q+1)/3$. If $m_2 = (q+1)/4 + d$ where $d \leq (q + 1)/12$, then $m_3 \geq (q + 1) - 2m_2 = (q + 1)/2 - 2d$, so

$$m_2(m_3 - 1) \geq \left(\frac{q+1}{4} + d\right)\left(\frac{q+1}{2} - 2d - 1\right) = \frac{q^2 - 1}{8} - 2d^2 - d \geq \frac{(q+1)^2}{9} - \frac{q+1}{3}.$$

Hence

$$2(q - 2) \geq m_2(m_3 - 1) \geq \frac{(q+1)^2}{9} - \frac{q+1}{3}.$$

This implies $q \leq 17$. For $q = 17$, equality occurs if and only if $m_1 = m_2 = m_3 = (q + 1)/3 = 6$, and there are 6 bisecants of $\mathcal{S}$ through both P_1 and P_2. This would mean that all of the lines joining these two points and the points of $\mathcal{S} \cap CP_3$ are bisecants. Thus there would be no tangent lines to $\mathcal{S}$ at the points $\mathcal{S} \cap CP_3$, contradicting the definition of semiovals. ■

It is well-known, that PG$(2, q)$ admits a cyclic Singer collineation group. This group is isomorphic to $\mathbb{Z}_{q^2+q+1}$, and it acts regularly on the points and lines of PG$(2, q)$. We say that *a set of points is cyclic,* if it is the orbit of a point under a subgroup of a Singer group. Batten and Dover [3] found a cyclic semioval in PG$(2, 7)$. It follows from our computer search, that this semioval is projectively unique. Hence we have the following theorem.

Theorem 14. *If $\mathcal{S}$ is a semioval in PG(2, 7) then $|\mathcal{S}| \leq 19$. If $|\mathcal{S}| = 19$, then $\mathcal{S}$ is cyclic.* ■

Cyclic semiovals are rare objects. There are only two known examples. For their investigation we use a non-classical embedding of PG$(2, q)$ into PG$(2, q^3)$. We briefly summarize it, the detailed description can be found in [5]. Let a be a primitive $(q^2 + q + 1)$-st root of unity in GF(q^3). Then PG$(2, q)$ can be embedded into PG$(2, q^3)$ in the following way: the points of PG$(2, q)$ are the elements of the set

$$\{P_i = (a^i, a^{(q+1)i}, 1) : i = 0, 1, 2, \ldots, q^2 + q\},$$

the lines of PG$(2, q)$ are the elements of the set

$$\{\ell_t = [t, t^{q+1}, 1] : t^{q^2+q+1} = 1\}.$$

The point P_i is incident with the line ℓ_t if and only if $ta^i + t^{q+1}a^{(q+1)i} + 1 = 0$. We say that ℓ_t has equation $tX + t^{q+1}Y + 1 = 0$.

Theorem 15. *There is no cyclic semioval in PG $(2, q)$ if $q \equiv 2 \pmod 3$.*

Proof. Suppose that $\mathcal{S}$ is a cyclic semioval in PG$(2, q)$. Then there exist integers k and m such that $km = q^2 + q + 1$, and

$$S = \{P_0, P_m, P_{2m}, \ldots, P_{(k-1)m}\}.$$

The transformation ϕ

$$P_i \mapsto P_{qi}, \qquad \ell_t \mapsto \ell_{t^q}$$

is a collineation of PG(2, q), because it maps points to points, lines to lines, and preserves the incidence, because

$$P_i \mathrm{I} \ell_t \iff ta^i + t^{q+1}a^{(q+1)i} + 1 = 0 \iff s\left(ta^i + t^{q+1}a^{(q+1)i} + 1\right)^q = 0 \iff$$
$$t^q a^{qi} + t^{q(q+1)}a^{q(q+1)i} + 1 = 0 \iff P_{qi} \mathrm{I} \ell_{t^q}.$$

This collineation preserves $\mathcal{S}$, because if $P_i \in \mathcal{S}$, then $P_{qi} \in \mathcal{S}$, and it has order three, because $d^{q^3} = d$ holds for all elements of $GF(q^3)$.

The point $P_0 = (1, 1, 1)$ is in $\mathcal{S}$, and $\phi(P_0) = P_0$. The line ℓ_t contains P_0 if and only if $t^{q+1} + t + 1 = 0$. Suppose that ℓ_t is the unique tangent to $\mathcal{S}$ at P_0. Then $\phi(\ell_t) = \ell_{t^q}$ also contains P_0 but does not contain any other point of $\mathcal{S}$. Hence it is also tangent to $\mathcal{S}$ at P_0. The tangent line is unique, hence $t = t^q$, and so $t^{q-1} = 1$. But $t^{q^2+q+1} = 1$ also holds, and from these two equations we get $t^3 = 1$. If $q \equiv 2 \pmod 3$, then $q^2 + q + 1$ is not divisible by 3, so $t \neq t^q$, hence in this case if $\mathcal{S}$ has one tangent at P_0, then it has at least three distinct tangents at the point P_0, so $\mathcal{S}$ could not be a semioval. ■

If $q = 3^r$, then it follows from the previous calculation, that the only possibility for $\mathcal{S}$ being a semioval is that the equation of the tangent line at P_0 is $X + Y + 1 = 0$. Computer search for $r \leq 11$ shows that it happens only for $r = 4$, hence if PG(2, 3^r) contains a cyclic semioval and $r \leq 11$, then $r = 4$ and $\mathcal{S}$ has 511 points.

Acknowledgements

The first author's research was supported by the Hungarian National Foundation for Scientific Research, Grant No. NK 67867, and by the Slovenian-Hungarian Intergovernmental Scientific and Technological Cooperation Project, Grant No. SI-2/2007. The second and third authors research was supported by the Italian MIUR (progetto 40% "Strutture Geometriche, Combinatoria e loro Applicazioni"), and by GNSAGA.

References

[1] S.C. Baker, G.L. Ebert, Intersection of unitals in the Desarguesian plane, Congr. Numer. 70 (1990) 87–94.
[2] L.M. Batten, Determining sets, Australas. J. Combin. 22 (2000) 167–176.
[3] L.M. Batten, J.M. Dover, Blocking semiovals of type $(1, m + 1, n + 1)$, SIAM J. Discrete Math. 14 (2001) 446–457.
[4] A. Blokhuis, Characterization of seminuclear sets in a finite projective plane, J. Geom. 40 (1991) 15–19.
[5] A. Cossidente, G. Korchmáros, The algebraic envelope associated to a complete arc, Rend. Circ. Mat. Palermo (2) Suppl. 51 (1998) 9–24.
[6] S.D. Cohen, Clique numbers of Paley graphs, Quaest. Math. 11 (1988) 225–231.
[7] J.M. Dover, Semiovals with large collinear subsets, J. Geom. 69 (2000) 58–67.
[8] A. Gács, On regular semiovals, J. Algebraic Combin. 23 (2006) 71–77.
[9] A. Gács, T. Szőnyi, Random constructions and density results, Des. Codes Cryptogr. 47 (2007) 267–287.
[10] J.W.P. Hirschfeld, T. Szőnyi, Sets in a finite plane with few intersection numbers and a distinguished point, Discrete Math. 97 (1991) 229–242.
[11] X. Hubaut, Limitation du nombre de points d'un (k, n)-arc regulier d'un plan projectif fini, Atti. Accad. Naz. Lincei Rend. 8 (1970) 490–493.
[12] Gy. Kiss, Small semiovals in PG(2, q), J. Geom. 88 (2008) 110–115.
[13] Gy. Kiss, S. Marcugini, F. Pambianco, Semiovals in projective planes of small order, in: Proceedings of Algebraic and Combinatorial Coding Theory, Eleventh International Workshop, Pamporovo, Bulgaria, 2008, pp. 151–154.
[14] Gy. Kiss, J. Ruff, Notes on small semiovals, Ann. Univ. Sci. Budapest. 47 (2004) 143–151.
[15] P. Lisonek, Computer-assisted Studies in Algebraic Combinatorics, Ph.D. Thesis, RISC, J. Kepler University Linz, 1994.
[16] H.B. Mann, Addition Theorems, John Wiley, 1965.
[17] C. Suetake, Some blocking semiovals which admit a homology group, European J. Combin. 21 (2000) 967–972.
[18] T. Szőnyi, Note on the existence of large minimal blocking sets in Galois planes, Combinatorica 12 (1992) 227–235.
[19] J.A. Thas, On semiovals and semiovoids, Geom. Dedicata 3 (1974) 229–231.